Domain: Security

DESCRIPTION

The Security Domain addresses the approach, methodology and technology components necessary to provide the appropriate level of protection for the information assets of the Commonwealth, its constituents and business partners. Security is a crosscutting component of the architecture that impacts every other Domain.

Although security requirements exist across all computing models, e.g. client/server and Web Services, the application of these security requirements on Web Services is different. For example, since SOAP messages can move across multiple legs of a communication link, a transport-centric authentication technique (such as SSL) is insufficient to assure data integrity and confidentially across the multiple "hops". The security context is lost as SOAP messages are routed between end-points.

STRATEGIC IMPORTANCE

The application of appropriate security protections for information technology is instrumental in fostering trust between government and its constituents and business partners. As a steward of public funds and public information, the Commonwealth has a responsibility to protect its information technology infrastructure and information assets.

The specific manner in which government Web Services are secured is critical to creating an Enterprise Service Oriented Architecture where:

- Information privacy and integrity is insured
- Different security systems can interoperate
- Enterprise security can be managed in an integrated fashion
- Platform independence can be achieved

RELATED TRENDS

- The traditional paradigm for information systems security - centralized, hierarchical and based on control – is increasingly in conflict with decentralized information resources over which the organization has limited ownership or control.
- What used to be a physical enterprise security perimeter is now becoming a logical enterprise security perimeter.
- With the advent of web services and increased communication and collaboration between the enterprise and external stakeholders, security is increasingly focusing on server-to-server security.
- XML-Aware (XAN) devices that are capable of parsing and processing XML documents are augmenting network level security devices.
- The identity security layer is being abstracted from applications so it can be managed in a more efficient, coordinated manner.

VISION

The Commonwealth's security architecture is enabling, yet non-intrusive. It ensures enterprise-wide interoperability as well as connectivity and collaboration with external stakeholders while providing appropriate protection to the state's information assets and infrastructure.

Service Oriented Architecture calls for information sharing on an enterprise and inter-enterprise scale, from government to business partner to employee. Sharing and interoperating among agencies, businesses and governments creates opportunities to improve the overall performance of government. Secure interoperability, based on identity management solutions, enables substantial cost savings, streamlined processes, and faster communication of vital information to the benefit of governments, businesses and citizens of the Commonwealth.

At the core of the Enterprise Service Oriented Architecture is the concept of Identity Management and the need for a standard that is open, interoperable and federated. In addition, it must allow for privacy safeguards across all sectors. The ETRM SOA Security Domain vision for the Commonwealth addresses:

- Open interoperability standards
- Federated Identities
- Centrally coordinated Governance
- Decentralized deployment

ROADMAP

Current State

- Emphasis is on network level security utilizing firewalls and public access architectures to protect servers within the enterprise
- Security policies are applied at the perimeter of an organization
- Each application develops and maintains its own unique identity and access security mechanisms

Target State

- A layered security model is implemented. Server-to-server security supplements network level security
- Granular security policies are applied above the network layer to enable "loosely coupled but tightly contracted" applications
- Identity and access security controls are abstracted from, and are external to, the application.
- Security services are provided by reusable components, providing a consistent and coordinated method of authentication and access control

- The creation of an Enterprise Registry Shared Service, to facilitate the management of security policy dissemination and enforcement across the enterprise

BOUNDARY

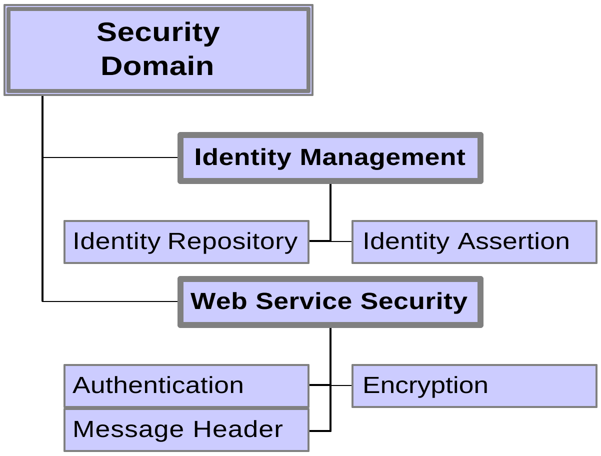
The Security Domain is associated with all other Domains because security concerns impact every layer of the architecture. The Security Domain does not directly address privacy considerations but has a role to play in implementing privacy protections for electronic data and systems.

RELATED POLICIES

- Enterprise Information Security Policy
- Enterprise Remote Access Security Policy

ASSOCIATED DISCIPLINES

- Identity Management
- Web Service Security



Domain: Security

Discipline: Identity Management

DESCRIPTION

Identity Management is a broad administrative area that deals with identifying individuals in a system and controlling their access to resources within that system by associating user rights and restrictions with the established identity. The driver licensing system is a simple example of identity management: drivers are identified by their license numbers and user specifications (such as "can not drive after dark") are linked to the identifying number.

In a wider context, industry standards groups such as the World Wide Web Consortium and OASIS are developing standards that would enable global identity management, in which each individual would be uniquely identified, and all applicable data would be linked to that identity

RELEVANT STANDARDS ORGANIZATIONS

- **OASIS** – The organization for advancement of structured information standards (OASIS) is currently working two sets of Service Registry standards, i.e. UDDI and ebXML. More information about OASIS can be found at http://www.oasis-open.org
- **W3C** - The World Wide Web Consortium was created in October 1994 to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. W3C has around 400 Member organizations from all over the world and has earned international recognition for its contributions to the growth of the Web. More information about W3C can be found at http://www.w3.org
- **WS-Interoperability –** The Web Services Interoperability Organization is an open industry effort chartered to promote Web Services interoperability across platforms, applications, and programming languages. More information about WS-I can be found at http://www.ws-i.org
- **IETF** - The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). More information on the IETF can be found at http://www.ietf.org/home.html.

STAKEHOLDERS/ROLES

- external and internal users of government information and services
- business service architects
- business analysts

- application developers

ROADMAP

User Ids and passwords are currently the most common form of end user authentication. Some secretariats and agencies are beginning the planning and/or migration to standards based Identity Management Systems. ITD has begun a major strategic effort to provide Identity Management Federation services at the enterprise level. The goal is to enable appropriate Commonwealth applications to support cross-domain authentication assertions, using open standards. We will also develop application layer security strategies, to complement existing network perimeter security strategies.

ENTERPRISE TECHNOLOGY SOLUTION

ITD is developing an Enterprise Identity Management Shared Service.

ASSOCIATED TECHNOLOGY AREAS

- Identity Repository
- Identity Assertion

Domain: Security

Discipline: Identity Management

Technology Area: Identity Repository

DESCRIPTION

An identity repository is a standards-based, special purpose, database or directory, for storing the information elements that comprise an entity's identity.

An Identity Repository is the place where unique identities for entities requiring Authentication are stored. Although this type of Repository is typically built on some proprietary database technology, the interfaces and schema must be Open Standards based. With this standards based interface approach, any business application, regardless of platform, will be able to leverage the Authentication Services provided by the Identity Repository.

Most large enterprises have dozens of identity repositories or directories which can be consolidated into standards based repositories, thus facilitating Single Sign On across multiple applications and systems.

TECHNOLOGY SPECIFICATION: LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

Description –LDAP is a client-server protocol for accessing a directory service, defined by the Internet Engineering Task Force (IETF). It was initially used as a front-end to X.500, but can also be used with stand-alone and other kinds of directory servers. The LDAP information model is based on the entry, which contains information about some object (e.g., a person). Entries are composed of attributes, which have a type and one or more values. Each attribute has a syntax that determines what kinds of values are allowed in the attribute and how those values behave during directory operations.

Guidelines – Application development projects should look to externalize authentication processes using the LDAP standard directory. Owners of existing systems and/or applications which utilize standalone proprietary identity repositories should analyze the cost benefits of an integrated standards based repository. Some of these benefits include single sign on and the ability to participation in an Identity Federation.

Standards and Specifications –

- Lightweight Directory Access Protocol (LDAP) v. 3.0

  Refer to: http://www.ietf.org/home.html

Migration Guidelines – Application development projects should begin to look to externalize authentication processes to facilitate a migration to a Lightweight Directory Access Protocol (LDAP) standard directory. Identify existing systems which utilize proprietary identity repositories, and obtain vendor roadmap for LDAP migration. Insure that procurement requirements for all new systems and/or applications provide LDAP V3 support.

Domain: Security

Discipline: Identity Management

Technology Area: Identity Assertion

DESCRIPTION

An Identity Assertion is a piece of data regarding either an act of authentication performed on a *subject*, attribute information about the subject, or authorization permissions applying to the subject with respect to a specified *resource*.

TECHNOLOGY SPECIFICATION: SECURITY ASSERTION MARKUP LANGUAGE (SAML)

Description **–** The Security Assertion Markup Language (SAML) is a standard framework for exchanging authentication and authorization information. Security typically involves checking the credentials presented by a party for authentication and authorization. SAML standardizes the representation of these credentials in an XML format called assertions, enhancing the interoperability between disparate applications. SAML makes use of XML-based assertions that contain credentials signed by a trusted authority.

Guidelines – SAML should be employed when an enterprise requires cross-domain single sign on to an external entity, e.g. business or government. SAML facilitates inter-enterprise sharing of information about users by authenticating and authorizing the user via security assertions, before allowing them access. Following these guidelines, Agencies do not have to maintain duplicate information about users.

Standards and Specifications –

- Security Assertion Markup Language (SAML) v. 1.1

  Refer to: http://www.oasis-open.org

Migration Strategy - Migration to SAML can be achieved by selecting or upgrading existing systems for support of this industry open standard. As an alternative, tool kits are available for SAML enabling legacy systems. In addition, trust relationships, e.g. contracts, and site-to-site authentication, must be established with entities with which cross-domain single sign on is desired, prior to SAML implementation.

Domain: Security

Discipline: Web Service Security

DESCRIPTION

Web Services that are exposed through a firewall are liable to be attacked if they are not properly secured with appropriate levels of authentication. Security Officers need to create and enforce message level security policies that guard against unauthorized use of Web Services.

SSL certificates and HTTP username/password are used per application session to grant access to a specific set of screens or Web pages – usually based on roles, responsibilities and privileged groups. This type of application-level authorization is session-oriented, and has no notion of granular access control to "application functionality". As a result, individual SOAP/XML messages and WSDL files are not checked for inappropriate content.

Trust-related vulnerabilities associated with Web Services are addressed by protecting the SOAP messages themselves. This can be accomplished by applying authentication to security tokens within SOAP messages or by signing and then attaching a digital signature to the SOAP message request. This form of persistent, embedded message security is enabled by SOA standards such as WS-Security, XML Signature and XML Encryption.

The WS-Interoperability group's Basic Security Profile is an interoperability profile that addresses SOAP messaging security and other security considerations for the Basic Profile 1.0, as well as the Basic Profile 1.1, Simple SOAP Binding Profile 1.0 and Attachments Profile 1.0, currently available for public review as Working Group Drafts. The Basic Security Profile is intended to work with other WS-I profiles and will reference existing specifications used to provide security, including the OASIS Web Services Security 1.0 specification, as well as provide clarifications and guidance designed to promote interoperability of those specifications.

RELEVANT STANDARDS ORGANIZATIONS

- **OASIS** – The organization for advancement of structured information standards (OASIS) is currently working two sets of Service Registry standards, i.e. UDDI and ebXML. More information about OASIS can be found at http://www.oasis-open.org
- **W3C** - The World Wide Web Consortium was created in October 1994 to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. W3C has around 400 Member organizations from all over the world and has earned international recognition for its contributions to the growth of the Web. More information about W3C can be found at http://www.w3.org
- **WS-Interoperability –** The Web Services Interoperability Organization is an open industry effort chartered to promote Web Services interoperability across platforms, applications, and programming languages. More information about WS-I can be found at http://www.ws-i.org

- **IETF** - The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). More information on the IETF can be found at http://www.ietf.org/home.html.

STAKEHOLDERS/ROLES

- external and internal users of government information and services
- business service architects
- business analysts
- application developers

ROADMAP

At the present time, authentication and encryption is applied at the network level. The Commonwealth has just begun developing and deploying Web Services. Traditional firewalls do not provide adequate protection for Web Services.

Trust-related vulnerabilities associated with Web Services need to be addressed by protecting the SOAP messages themselves. Web Service application level security policies will be developed and enforced.

ENTERPRISE TECHNOLOGY SOLUTION

ITD is developing an XML Gateway Shared Service which can provide XML schema validation as well as message authentication and encryption based on open standards.

ASSOCIATED TECHNOLOGY AREAS

- Web Service Authentication
- Web Service Encryption
- Web Service Message Header

Domain: Security

Discipline: Web Service Security

Technology Area: Web Service Authentication

DESCRIPTION

Web Service Authentication is a mechanism for ensuring the origin and integrity of XML documents. Web Services are, by their nature, message-oriented and lack the guarantee of a direct connection between service provider and consumer. Therefore, traditional connection-oriented security approaches are insufficient because a connection-oriented protocol cannot guarantee confidentiality between a message's initial producer and its final consumer.

TECHNOLOGY SPECIFICATION: XML SIGNATURE

Description - XML Signature standardizes the process of signing XML content and inserting it into XML documents, so that recipients can verify its origin and integrity. XML Signature provides an electronic method for stamping an identity onto XML content. Recipients of this XML content can then examine the stamp to ensure that the content was, in fact, created and sent by the expected sender. This stamp further provides the recipient with assurance that the XML content remained intact and unchanged while in transit. When combined with appropriate logging, XML signatures provide evidence of the origin of messages that can be used to resolve transaction disputes between parties.

Guidelines – Use XML Signature whenever there is a business requirement for Web Service message level authentication. In addition, XML Signature is recommended when a message must traverse multiple enterprise boundaries before reaching the destination application, i.e. network layer authentication is point to point in nature, and will not traverse inter-network boundaries.

Standards and Specifications –

- XML Signature - An open standard developed by the W3C. XML Signature is also specified by WS-Interoperability as part of its draft Basic Security Profile, and is the Commonwealth’s baseline standard for Web Service authentication.
  Refer to: http://www.w3.org/Signature/

Migration Strategy – XML Signature migration must be considered as part of a strategy to migrate to XML based application services. To facilitate a migration to XML Signature, policies for the optional use of digital certificate authentication will need to be developed.

Domain: Security

Discipline: Web Service Security

Technology Area: Encryption

DESCRIPTION

Encryption is based on two components: an algorithm and a key. A cryptographic algorithm is a mathematical function that takes intelligible information (plain text) as input and changes it into unintelligible cipher text. In order to encrypt the plain text, most algorithms use a key as input in conjunction with an encryption formula. Both the key and the function used are crucial to the encryption -- the same key used in two different encryption functions will produce two different results, and two keys used with the same function also produce two different results. The number of possible keys each algorithm can support depends on the number of bits in the key.

Web Service Encryption provides end-to-end security for applications that require secure exchange of structured data. XML itself is the most popular technology for structuring data, and therefore XML-based encryption is the natural way to handle complex requirements for security in data interchange applications.

TECHNOLOGY SPECIFICATION: XML ENCRYPTION

Description – The World Wide Web Consortium (W3C) has announced the publication of *XML Encryption Syntax and Processing* and *Decryption Transform for XML Signature*, signifying a cross-industry agreement on an XML-based approach for securing XML data in a document.

Guidelines – Message-level encryption is necessary when transactions use inter-enterprise intermediaries for security, caching, routing, and transaction management. Typically, these intermediaries examine the public information contained in the messages that will perform each function. Content-level encryption is also useful when messages contain private data. Public data remains as plaintext when sent over the wire so intermediaries can examine it. Private data, such as patient information and social security numbers, is encrypted into and represented by cipher text until the destination application receives it. Use XML Encryption when there is a requirement for message level encryption from Service End-Point to Service End-Point. With this approach data is not decrypted until it reaches its final end-point destination.

Standards and Specifications –

- XML Encryption – An open standard developed by the W3C. XML Encryption is also specified by WS-Interoperability as part of its draft Basic Security Profile, and is the Commonwealth's baseline standard for providing message level encryption.
  Refer to: http://www.w3.org/Encryption/2001/

***Migration Strategy* –** Any XML Encryption migration strategy must first address migration to XML based application services, and XML Signature. XML Encryption requires XML Signature to provide the asymmetric keys used to implement XML Encryption.

Domain: Security

Discipline: Web Service Security

Technology Area: Web Service Message Header

DESCRIPTION

The Web Service Message Header Technology Area addresses open standards for embedding security information into SOAP messages. While SOAP provides a flexible technique for structuring messages, it does not directly address how to secure these messages. WS-Security builds upon the SOAP specification, structuring the use of essential security capabilities. Specifically, WS-Security uses security tokens for authentication, digital signatures for integrity, and content-level encryption for confidentiality. By structuring SOAP security, WS-Security makes it easy to include security elements into SOAP through tools and enterprise applications. This specification provides a general-purpose mechanism for associating security tokens with message content. It should be noted that no specific type of security token is required, the specification is designed to be extensible (i.e. support multiple security token formats, including passwords).

TECHNOLOGY SPECIFICATION: WS-SECURITY

Description - WS-Security builds upon the SOAP header extensions, providing explicit headers that contain binary security tokens, digital signatures according to the XML Signature specification, and content-level encryption according to the XML Encryption specification.

Guidelines – WS-Security is most valuable in the context of external integration with partners or internal integration between geographically dispersed applications. In both cases, applications exchange messages in the open network, exposing the parties to numerous threats. Several security capabilities must be used to secure the message flow.

Standards and Specifications –

- WS-Security 1.0– An open standard developed by OASIS. It is also specified by WS-Interoperability as part of its draft Basic Security Profile, and is the Commonwealth's baseline standard for the format of SOAP message headers that specify authentication and encryption to be provided.
  Refer to: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

Migration Strategy – Since WS-Security is SOAP based, it implies a migration to SOAP based application services as a prerequisite to WS-Security deployment. Both XML Signature and XML Encryption can be used with XML, prior to SOAP deployment, and therefore provide a migration path to WS-Security.